

## **AMENDMENTS TO THE CLAIMS**

Please amend the claims of the present application as set forth below. In accordance with the PTO's revised amendment format, a detailed listing of all claims has been provided. This listing of claims will replace all prior versions and listings of claims in the application. Changes to the claims are shown by strikethrough (for deleted matter) and underlining (for added matter).

By way of overview claims 1-2 and 4-42 are currently pending. More specifically, the status of the claims is indicated below:

- a) Claims 1, 4 and 6 are currently amended;
- b) Claims 2, 5 and 7-39 are original;
- c) Claim 3 is canceled without prejudice or disclaimer; and
- d) Claims 40-42 are new.

## **Listing of Claims**

1. (Currently amended) A system comprising:

a pluggable security policy enforcement module configured to be replaceable in the system and to provide different granularities of control for a business logic in the system, wherein the business logic processes requests submitted to the system,

wherein the pluggable security policy enforcement module is configured to determine, for a particular granularity of control, whether to permit an operation, requested by a user based at least in part on a permission assigned to the user.

2. (Original) A system as recited in claim 1, wherein the different granularities of control comprise a plurality of sets of rules that can be replaced with each other without altering the business logic.

1  
2       3. (Cancelled)

3  
4       4. (Currently Amended) A system ~~as recited in claim 1, comprising:~~  
5       a pluggable security policy enforcement module configured to be replaceable in  
6       the system and to provide different granularities of control for a business logic in the  
7       system, wherein the business logic processes requests submitted to the system.

8       wherein the pluggable security policy enforcement module includes a control  
9       module configured to determine whether to permit an operation based at least in part on  
10       accessing the business logic to identify one or more additional tests to perform, and  
11       further configured to perform the one or more additional tests.

12  
13       5. (Original) A system as recited in claim 4, wherein the control module is further  
14       configured to return a result of the determining to the business logic.

15  
16       6. (Currently amended) A system ~~as recited in claim 1, comprising:~~  
17       a pluggable security policy enforcement module configured to be replaceable in  
18       the system and to provide different granularities of control for a business logic in the  
19       system, wherein the business logic processes requests submitted to the system,

20       wherein the different granularities of control comprise a plurality of sets of rules,  
21       and wherein each set of rules includes a plurality of permission assignment objects,  
22       wherein each of the permission assignment objects associates a user with a particular  
23       role, wherein each particular role is associated with one or more permissions, and  
24       wherein each of the one or more permissions identifies a particular operation and context  
25       on which the operation is to be performed.

1  
2       7. (Original) A system as recited in claim 6, wherein each of the permission  
3 assignment objects further identifies whether the one or more permissions in the  
4 particular role are granted to the user or denied to the user.

5  
6       8. (Original) One or more computer-readable media comprising computer-  
7 executable instructions that, when executed, direct a processor to perform acts including:

8           receiving a request to perform an operation;  
9            checking whether to access a business logic in order to generate a result for the  
10          requested operation;

11           obtaining, from the business logic, a set of zero or more additional tests to be  
12          performed in order to generate the result;

13           performing each additional test in the set of tests if there is at least one test in the  
14          set of tests;

15           checking a set of pluggable rules to determine the result of the requested  
16          operation; and

17           returning, as the result, a failure indication if checking the business logic or  
18          checking the set of pluggable rules indicates that the result is a failure, otherwise  
19          returning, as the result, a success indication.

20  
21        9. (Original) One or more computer-readable media as recited in claim 8, wherein  
22          the receiving comprises receiving, from the business logic, the request to perform the  
23          operation.

1       10. (Original) One or more computer-readable media as recited in claim 8,  
2       wherein the receiving comprises receiving, as part of the request, an indication of a user,  
3       and wherein the checking the set of pluggable rules comprises comparing an object  
4       associated with the user to the rules in the set of pluggable rules and determining whether  
5       the operation can be performed based at least in part on whether the user is permitted to  
6       perform the operation.

7  
8       11. (Original) One or more computer-readable media as recited in claim 8,  
9       wherein the receiving comprises having one of a plurality of methods invoked.

10  
11      12. (Original) One or more computer-readable media as recited in claim 8,  
12       wherein the set of pluggable rules is a set of security rules defined using high-level  
13       permission concepts.

14  
15      13. (Original) One or more computer-readable media as recited in claim 12,  
16       wherein the high-level permission concepts include an operation and a context, wherein  
17       the operation allows identification of an operation to be performed and the context allows  
18       identification of what the operation is to be performed on.

19  
20      14. (Original) One or more computer-readable media as recited in claim 8,  
21       wherein the computer-executable instructions are implemented as an object.

22  
23      15. (Original) One or more computer-readable media as recited in claim 8,  
24       wherein the computer-executable instructions further direct the processor to perform acts  
25       including:

1       determining if at least one of the tests in the set of zero or more additional tests  
2       would indicate a result of failure; and

3               returning, as the result, the failure indication without checking the set of  
4       pluggable rules.

5  
6       16. (Original) One or more computer-readable media as recited in claim 8,  
7       wherein the set of pluggable rules can be replaced with another set of pluggable rules  
8       without altering the business logic.

9  
10       17. (Original) One or more computer-readable media as recited in claim 8,  
11       wherein the set of pluggable rules includes a plurality of permission assignment objects,  
12       wherein each of the permission assignment objects associates a user with a particular  
13       role, wherein each particular role is associated with one or more permissions, and  
14       wherein each of the one or more permissions identifies a particular operation and context  
15       on which the operation is to be performed.

16  
17       18. (Original) One or more computer-readable media as recited in claim 17,  
18       wherein each of the permission assignment objects further identifies whether the one or  
19       more permissions in the particular role are granted to the user or denied to the user.

20  
21       19. (Original) A method comprising:  
22               providing high-level permission concepts for security rules;  
23               allowing a set of security rules to be defined using the high-level permission  
24       concepts, wherein the set of security rules allows permissions to be assigned to users of  
25       an application; and

1       determining, based at least in part on a permission assigned to a user, whether to  
2 permit an operation based on a request by the user.

3  
4       20. (Original) A method as recited in claim 19, wherein the determining further  
5 comprises determining whether to permit the operation requested by the user based at  
6 least in part on accessing a business logic to identify one or more additional tests to  
7 perform, and further comprising performing the one or more additional tests.

8  
9       21. (Original) A method as recited in claim 20, further comprising returning a  
10 result of the determining to the business logic.

11  
12       22. (Original) A method as recited in claim 19, wherein the high-level permission  
13 concepts include an operation and a context, wherein the operation allows identification  
14 of an operation to be performed and the context allows identification of what the  
15 operation is to be performed on.

16  
17       23. (Original) A method as recited in claim 19, wherein the method is  
18 implemented in an object having a plurality of interfaces for requesting a determination  
19 as to whether to permit a plurality of operations including the operation requested by the  
20 user.

21  
22       24. (Original) A method as recited in claim 19, wherein the set of security rules  
23 includes a plurality of permission assignment objects, wherein each of the permission  
24 assignment objects associates a user with a particular role, wherein each particular role is  
25 associated with one or more permissions, and wherein each of the one or more

1 permissions identifies a particular operation and context on which the operation is to be  
2 performed.

3  
4 25. (Original) A method as recited in claim 24, wherein each of the permission  
5 assignment objects further identifies whether the one or more permissions in the  
6 particular role are granted to the user or denied to the user.

7  
8 26. (Original) A method comprising:  
9 receiving a request to perform an operation;  
10 accessing a set of low-level rules, wherein the low-level rules are defined in terms  
11 of high-level concepts;  
12 checking whether a user requesting to perform the operation is entitled to perform  
13 the operation based at least in part on the set of low-level rules; and  
14 returning an indication of whether the operation is allowed or not allowed.

15  
16 27. (Original) A method as recited in claim 26, wherein the checking further  
17 comprises checking whether the user is entitled to perform the operation based at least in  
18 part on accessing a business logic to identify one or more additional tests to perform, and  
19 further comprising performing the one or more additional tests.

20  
21 28. (Original) A method as recited in claim 27, wherein the set of low-level rules  
22 can be replaced with another set of low-level rules without altering the business logic.

23  
24 29. (Original) A method as recited in claim 27, further comprising returning the  
25 indication to the business logic.

1

2 30. (Original) A method as recited in claim 26, wherein the low-level rules  
3 include a plurality of permission assignment objects, wherein each of the permission  
4 assignment objects associates a user with a particular role, wherein each particular role is  
5 associated with one or more permissions, and wherein each of the one or more  
6 permissions identifies a particular operation and context on which the operation is to be  
7 performed

8

9 31. (Original) A method comprising:  
10 assigning high level security concepts to an application domain; and  
11 allowing a set of pluggable rules to define low-level rules, in terms of the high  
12 level security concepts, for different business logic in the application domain.

13

14 32. (Original) A method as recited in claim 31, wherein the high level security  
15 concepts include an operation and a context that identifies what the operation is  
16 performed on.

17

18 33. (Original) A method as recited in claim 31, further comprising:  
19 determining, based at least in part on a permission assigned to a user and on one  
20 or more additional tests identified by accessing the business logic, whether to permit an  
21 operation based on a request by the user

22

23 34. (Original) A method as recited in claim 33, further comprising returning a  
24 result of the determining to the business logic.

25

1           35. (Original) An architecture comprising:  
2           a plurality of resources;  
3           a business logic layer to process, based at least in part on the plurality of  
4 resources, requests received from a client; and  
5           a pluggable security policy enforcement module to enforce security restrictions on  
6 accessing information stored at the plurality of resources.

7  
8           36. (Original) An architecture as recited in claim 35, wherein the pluggable  
9 security policy enforcement module defines high-level permission concepts for security  
10 rules and further defines a set of security rules using the high-level permission concepts.

11  
12          37. (Original) An architecture as recited in claim 36, wherein the high-level  
13 permission concepts include an operation and a context, wherein the operation allows  
14 identification of an operation to be performed and the context allows identification of  
15 what the operation is to be performed on.

16  
17          38. (Original) An architecture as recited in claim 35, wherein the pluggable  
18 security policy enforcement module can be replaced with another pluggable security  
19 policy enforcement module to enforce different security restrictions without altering the  
20 business logic layer.

21  
22          39. (Original) An architecture as recited in claim 35, wherein the pluggable  
23 security policy enforcement module is configured to determine, based at least in part on a  
24 permission assigned to a user and on one or more additional tests identified by accessing

1 the business logic layer, whether to permit an operation to access information at the  
2 plurality of resources.

3 40. (New) A system as recited in claim 1, wherein the system is configured as a  
4 multi-layer architecture, wherein the business logic is implemented as a business logic  
5 layer of the multi-layer architecture.

6

7 41. (New) A system as recited in claim 1, wherein the pluggable security policy  
8 enforcement module is configured to receive an input from the business logic in the form  
9 of a user indication and an item indication.

10

11 42. (New) A system as recited in claim 1, wherein the pluggable security policy  
12 module includes an interface that provides the following interface functionality:

13 first functionality for testing whether an identified item can be approved by a  
14 specified user;

15 second functionality for testing whether the identified item of a specified type can  
16 be created by the specified user;

17 third functionality for testing whether the identified item can be deleted by the  
18 specified user;

19 fourth functionality for testing whether the identified item can be modified by the  
20 specified user; and

21 fifth functionality for testing whether the identified user can examine details of  
22 the identified item.

23

24

25